HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Annamaria Nockemann

Online-Durchsuchung im Spannungsfeld zwischen Prävention und Repression

Mittweida, 2018

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Online-Durchsuchung im Spannungsfeld zwischen Prävention und Repression

Autor:
Frau

Annamaria Nockemann

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO14w1-B

Erstprüfer:
Prof. Dr. iur. Frank Czerner

Zweitprüfer:
Prof. Dr. rer. nat. Christian Hummert

Einreichung:
Sprockhövel, 01.10.2018

Verteidigung/Bewertung:
Mittweida, 2018

Faculty **Applied Computer and Life Sciences**

BACHELOR THESIS

Online search in the tension between prevention and repression

author:
Ms

Annamaria Nockemann

course of studies:
Allgemeine und Digitale Forensik

seminar group:
FO14w1-B

first examiner:
Prof. Dr. iur. Frank Czerner

second examiner:
Prof. Dr. rer. nat. Christian Hummert

submission:
Sprockhövel, 01.10.2018

defence/ evaluation:
Mittweida, 2018

Bibliografische Angaben

Nockemann, Annamaria: Online-Durchsuchung im Spannungsfeld zwischen Prävention und Repression, 32 Seiten, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften

Bachelorarbeit, 2018

Referat

Mit der zunehmenden Verbreitung moderner Technologien entsteht auch eine hohe Missbrauchsgefahr. Um eine effektive Gefahrenabwehr weiterhin gewährleisten zu können, erfordert es die Ausweitung der Befugnisse der Sicherheitsbehörden, bzw. die Anpassung an die technischen Möglichkeiten, durch die Schaffung neuer gesetzlicher Grundlagen, die nun für die Online-Durchsuchung erarbeitet wurden. Fraglich ist, ob sich die Argumente des präventiven so einfach auf den repressiven Einsatz dieser Maßnahme übertragen lassen. Ein weiteres, ungleich schwereres Problem ist die Verwendung von Sicherheitslücken zum Aufspielen der Maßnahme, vor allem bei der Repression, allerdings auch bei der Prävention. In diesem Zusammenhang stellt sich die Frage, ob die Ermittlungserkenntnisse im Strafprozess Beweiskraft besitzen.

Abstract

With the increasing use of modern technologies, there is also a high risk of abuse. In order to continue to ensure the effective protection against danger, it is necessary to extend the powers of the security authorities, or to adjust these according to the technical possibilities, by creating new legal bases, which have now been developed for the online search. It is questionable whether the arguments of the preventive use can easily be transferred to the repressive use of this measure. Another much more serious problem is the use of security vulnerabilities to deploy the measure, especially in repression, but also in prevention. In this context, the question arises as whether the investigative knowledge in criminal proceedings have evidential value.

Inhaltsverzeichnis

1 Einführung

Die Online-Durchsuchung als verdeckter Zugriff auf informationstechnische Systeme hat in den letzten Jahren zunehmend an Aufmerksamkeit gewonnen. Einst für präventive Zwecke eingeführt, um den internationalen Terrorismus zu bekämpfen, eröffnen sich damit inzwischen auch neue Möglichkeiten der Nutzung der Online-Durchsuchung in der Strafverfolgung. Gerade im Voranschreiten des digitalen Zeitalters und der Bedeutung informationstechnischer Systeme wächst auch die der digitalen Spuren.

Bereits Ende 2006 wurde in Nordrhein-Westfalen ein Gesetz verabschiedet, das das „heimliche Aufklären des Internets“ ermöglichte, Teil davon war auch die Maßnahme zur Durchführung der Online-Durchsuchung. Dies wurde allerdings vom Bundesverfassungsgericht für unzulässig erklärt. Trotz des Scheiterns dieses Gesetzes wurde die Notwendigkeit erkannt, Maßnahmen im Zuge des Voranschreitens von digitalen Spuren, verschlüsselten Kommunikationsmitteln und verschlüsselten Daten anzupassen oder entsprechende Grundlagen zu schaffen, vor allem unter der Bedeutung moderner Technologien für Personen, die Straftaten planen, aber auch Personen, die Straftaten bereits begangen haben. Im Jahr 2008 wurde dementsprechend eine Grundlage der Online-Durchsuchung im Bundeskriminalamtsgesetz (BKAG) geschaffen im Zuge der Aufgabenzuteilung, Gefahren des internationalen Terrorismus abzuwenden.

Die Auswirkungen der Online-Durchsuchung auf die Integrität und die Vertraulichkeit der informationstechnischen Systeme und damit auch der Daten, die sich auf den entsprechenden Datenträgern befinden, sind dabei nicht immer unmittelbar klar, in jedem Fall wird jedoch in die Freiheit des Einzelnen, bzw. in das Recht auf die freie Entfaltung seiner Persönlichkeit eingegriffen. Der Staat hat die Aufgabe, diese Freiheit vor Eingriffen Dritter oder des Staates selbst zu schützen. Es ist jedoch nicht in vollem Umfang möglich, die Freiheit des Einzelnen und den Schutz vor kriminellen und terroristischen Gefahren zu gewährleisten. Gegenüber einer effektiven Prävention und Repression stehen die Begriffe *Gläserner Mensch* und *Überwachungsstaat*, in dem Zusammenhang wird auch gerne gesagt „Ich habe nichts zu verbergen.“ oder „Wer nichts zu verbergen hat, hat auch nichts zu befürchten.“ Deshalb sind den Eingriffsmöglichkeiten in Form von Maßnahmen wie der Online-Durchsuchung Schranken zu setzen (und bereits gesetzt), sodass ihr Eingriff in die Rechte des Einzelnen verhältnismäßig bleibt. Es liegt auf der Hand, dass ein Kompromiss sowie das richtige Maß gefunden werden muss, denn ohne Eingriffe in Rechte von Einzelnen können auch keine Gefahren abgewendet werden.

Dennoch entsteht bei einigen Bürgern der Eindruck, dass eine immer stärkere Überwachung möglich ist, bzw. stattfindet, welche sich teilweise mit dem Sicherheitsaspekt be-

gründen lässt, teilweise aber auch zu einer Einschränkung bürgerlicher Freiheiten tendiert, die nicht mehr verhältnismäßig erscheint. Bei der gezielten Verheimlichung von Sicherheitslücken seitens staatlicher Behörden, die zum Aufspielen von Spionagesoftware auf ein informationstechnisches System genutzt werden, wird in Kauf genommen, dass Dritte diese Sicherheitslücken ebenfalls nutzen, statt dass die Behörden die Schwachstellen den entsprechenden Herstellern melden, die sie dann schließen können. Dies schürt die Unsicherheit und das Unverständnis der Bürger, sodass das Vertrauen in die Sicherheit des Internets und in den Staat selbst, dessen Aufgabe es sein sollte, für die Sicherheit zu sorgen, geschädigt wird.

Zielsetzung dieser Arbeit ist die Auseinandersetzung mit den rechtlichen und technischen Möglichkeiten und Grenzen der Online-Durchsuchung und vor allem die Beleuchtung der Probleme, die dabei auftreten, sowohl in Bezug auf die Rechtfertigung als auch hinsichtlich weiterführender Gefahren, die mit der Durchführung der Maßnahme auftreten. Zu fragen ist, ob der rechtliche Rahmen zu eng, angemessen oder zu weit gefasst ist. Des Weiteren geht diese Arbeit auf die parlamentarische sowie auch außerparlamentarische Diskussion zur Online-Durchsuchung sowohl zum Zweck der Prävention als auch zum Zweck der Repression ein. Unter Berücksichtigung der technischen Voraussetzungen und des Ablaufs wird auch die Missbrauchsgefahr durch unbefugte Dritte mit eingeschlossen.

2 Online-Durchsuchung

Bei der Online-Durchsuchung wird eine bestehende Verbindung zum Internet genutzt, um darüber heimlich auf ein informationstechnisches System zuzugreifen. Dabei kann ein einmaliger Zugriff auf das System und damit auf die gespeicherten Daten erfolgen, um nach bestimmten Dateien zu suchen oder eine Komplettkopie des Datenträgers erstellt werden, auch *Spiegelung* genannt, dies entspricht einer Durchsicht. Wenn Bereiche der Festplatte oder auch externe Datenträger jedoch verschlüsselt sind, bietet sich hingegen eine kontinuierliche Überwachung an, auch *Monitoring* genannt, um bei genügend langer Überwachungszeit des Rechners ebenfalls eine vollständige Spiegelung der Daten zu erhalten, da der Nutzer des informationstechnischen Systems „früher oder später den Zugriff freischalten“ wird.[1]

Der Zugriff auf ein informationstechnisches System erfolgt mit geeigneter und auf den Einzelfall angepasster Software, auf die ich in Abschnitt 2.2 genauer eingehen werde.

Voneinander zu unterscheiden sind die Zwecke des Einsetzens von Online-Durchsuchung: Prävention und Repression. Auf diese beiden werde ich im weiteren Verlauf meiner Arbeit eingehen.

2.1 Abgrenzung zur (Quellen-)Telekommunikationsüberwachung

Die Maßnahme der Telekommunikationsüberwachung umfasst die Überwachung und Aufzeichnung ausschließlich *laufender* Kommunikation und erfolgt ohne Wissen des Betroffenen. Unter den Begriff der Telekommunikation fallen hier u.a. das Abhören von Telefongesprächen und das Mitlesen von E-Mails, Kurzmitteilungen oder Telefaxen.

Durch die zunehmende Vielfalt und Komplexität von Kommunikationskanälen, vor allem auch durch die verbreitete Nutzung kryptografischer Verfahren[2] werden größere Anforderungen an die Überwachungsmaßnahmen gestellt, um noch effektiv eingesetzt werden zu können. Dabei müssen die Maßnahmen entweder immer umfassender gestaltet werden oder „immer näher an der Schnittstelle zwischen Mensch und Maschine ansetzen“, um die Verschlüsselung der Telekommunikationsinhalte zu umgehen.[3]

Heutzutage erfolgt ein Großteil der Kommunikation Internetprotokoll-(IP)-basiert und zahlreiche „Voice-over-IP“ (VoIP)- und Messenger-Dienste versehen ihre Kommunikati-

[1] Buermeyer [7, S. 160 f.]
[2] BT-Drs. 16/10121 [10, S. 28]
[3] Bundesregierung: Evaluationsbericht zu § 20k BKAG, 2017 [11, S. 39]

onsinhalte mit einer Verschlüsselung.[4] Wenn nun ein komplexes informationstechnisches System technisch infiltriert wird, um die laufende Kommunikation vor der Verschlüsselung oder nach der Entschlüsselung zu erfassen und zu überwachen, fällt das unter die sogenannte Quellen-Telekommunikationsüberwachung.[5]

Die Online-Durchsuchung hingegen ermöglicht den Zugriff auf Daten, die „noch nicht oder nicht mehr Gegenstand einer laufenden Telekommunikation sind oder überhaupt nicht für eine Telekommunikation vorgesehen sind." In dem Sinne kann auf alle gespeicherten, bzw. verfügbaren Daten eines informationstechnischen Systems zugegriffen werden. Nicht gestattet ist (bisher) allerdings der Zugriff auf Kameras oder Mikrofone, die zu den Hardware-Komponenten des Computers gehören.[6]

Da es bei dem Einsatz beider Maßnahmen zum heimlichen Zugriff auf informationstechnische Systeme und zur Ausleitung sowie Übermittlung von Daten kommt, weist die Online-Durchsuchung in ihrer Funktion Ähnlichkeiten zur Quellen-Telekommunikationsüberwachung auf. Eine Abgrenzung der Maßnahmen ist laut Bundesregierung erforderlich, da diese in unterschiedliche Grundrechte eingreifen. Durch eine hinreichende Trennung der Maßnahmen sei gewährleistet, dass es bei der Quellen-Telekommunikationsüberwachung nicht zur faktischen Online-Durchsuchung kommt.[7] Wenn also technisch sichergestellt werden kann, dass eine Überwachung bloß auf die laufende Kommunikation begrenzt ist, ist die Quellen-Telekommunikationsüberwachung erlaubt. Andernfalls müsse auf die Maßnahme der Online-Durchsuchung zurückgegriffen werden.[8]

Da die Quellen-Telekommunikation auf die Überwachung laufender Kommunikation zielt, ist sie allein an Art. 10 GG (Telekommunikationsgeheimnis) zu messen. Der Schutzbereich dieses Grundrechts ist dabei unabhängig von der Eingriffsstelle der Maßnahme, auf der Übertragungsstrecke oder am Endgerät der Telekommunikation, betroffen.[9]. Da die Online-Durchsuchung, wie bereits erläutert, keine Erweiterung der Quellen-Telekommunikationsüberwachung darstellt, ist diese Maßnahme nicht an Art. 10 GG, sondern durch Zugriff auf gespeicherte oder verfügbare Daten eines informationstechnischen Systems allein am Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 i. V. m. Art. 1 GG, auf welches im Verlauf meiner Arbeit noch näher eingegangen wird, zu messen. [10]

[4] Bundesregierung Formulierungshilfe zu § 100a [13, S. 18]
[5] BVerfG 27.2.2008 [14, Rn. 188]
[6] BT-Drs. 16/10121 [10, S. 28]
[7] Bundesregierung: Evaluationsbericht zu § 20k BKAG, 2017 [11, S. 39]
[8] BVerfG 20.4.2016 [15, Rn. 234]
[9] BVerfG 27.2.2008 [14, Rn. 184, 190]
[10] Bundesregierung Evaluationsbericht, 2017 [11, S. 39], vgl. auch BVerfG 20.4.2016 [15, Rn. 209]

Aus dem Urteil des Bundesverfassungsgerichtes vom 27. Februar 2008 über das nordrhein-westfälische Verfassungsschutzgesetz (VSG) geht hervor, dass mit der Umgehung von bestehenden Schutzmaßnahmen gegen Unbefugte und der im Anschluss folgenden Infiltration eines informationstechnischen Systems die entscheidende, technische Hürde zur Ausspähung des Systems insgesamt genommen ist.[11] Zwar unterscheiden sich Online-Durchsuchung und Quellen-Telekommunikationsüberwachung in Bezug auf die verwendete Software, aber nicht hinsichtlich der auszunutzenden vorhandenen Sicherheitslücken.[12]

[11] BVerfG 27.2.2008 [14, Rn. 188], vgl. auch Roggan [26, S. 1]
[12] Roggan [26, S. 1]

2.2 Technische Voraussetzungen und Ablauf

Bei der Online-Durchsuchung wird in ein „*informationstechnisches System*“ eingegriffen. Durch Verwendung dieser Formulierung wird bewusst verhindert, sich auf einen bestimmten Gerätetyp, bzw. ein bestimmtes Betriebssystem, eine Programmierung o.ä. festzulegen. Ein informationstechnisches System ist ein System, welches Daten „erheben, verarbeiten und die Ergebnisse ausgeben oder weiterleiten“ kann. Diese Formulierung ist für zukünftig entwickelte Geräte und Techniken ebenfalls offen. [13]

Die Online-Durchsuchung ist eine zeit- und vorbereitungsintensive Maßnahme. Für jeden einzelnen Fall soll eine spezielle Durchsuchungssoftware entwickelt, bzw. angepasst werden, entsprechend den „ermittlungstaktischen Bedürfnissen und [...] dem Umfang der gerichtlichen Anordnung.“[14]

Im Volksmund ist bei der Online-Durchsuchung oft von einem *Bundes-Trojaner* die Rede, dies ist eine Anlehnung an *Trojanische Pferde* oder auch *Trojaner* - Schadprogramme, die neben einer dem Anwender offen erkennbaren Funktion ihren eigentlichen Zweck verstecken,[15] um den Erfolg der Maßnahme nicht zu gefährden.[16] Dies setzt nicht immer die Aktivität des Nutzers voraus.

Um nun an die gespeicherten Daten auf dem informationstechnischen System zu gelangen, muss eine Software auf das zu infiltrierende informationstechnische System aufgespielt werden und dazu sowie zum Ausleiten und Übermitteln der Daten eine Verbindung zum Internet bestehen.[17]

Die Installation einer solchen Spionage-Software kann physisch vor Ort erfolgen, etwa bei einer Grenzkontrolle oder durch heimliches Betreten der Räumlichkeiten, in denen sich das informationstechnische System befindet.[18] Auch infrage kommt das Zuspielen eines Datenträgers mit der entsprechenden Software oder die Manipulation von Geräten auf dem Lieferweg. Die Installation einer Spionage-Software kann auch online erfolgen. Dazu gehört beispielsweise das Herunterladen oder Aktualisieren von Programmen, Drive-By-Infektionen, vor allem aber auch das Nutzen von Sicherheitslücken. Die Software muss Befehle empfangen, verarbeiten, Programmteile nachladen und Daten und Ergebnisse der Datenverarbeitung übermitteln können.[19] Nach Eindringen in das

[13] Graf [21, § 100b, Rn. 7]
[14] Bundesregierung: Evaluationsbericht zu § 20k BKAG, 2017 [11, S. 38]
[15] Buermeyer [7, S. 155]
[16] Skistims und Roßnagel [27, S. 3]
[17] Buermeyer [7, S. 155]
[18] Buermeyer, 2017 [8, S. 21]
[19] Roßnagel, Skistims, 2012 [27, S. 4]

System beginnt die Software in der Zeit, in der sie aktiv ist, nach ihrer Programmierung relevante Daten auf dem Computer zu sammeln und sendet diese an die Ermittler. Die Software ist im besten Fall so programmiert, dass sie alle relevanten Daten erfasst und übermittelt und nicht-relevante Daten ignoriert, da eine regelmäßig stattfindende Übertragung aller Daten nicht infrage kommt und zudem die nicht-relevanten Daten des Betroffenen geschützt werden sollen. Dazu muss eine Vorauswahl der zu übermittelnden Daten getroffen werden, welches sich als nicht ganz einfach herausstellt, da sich die Relevanz häufig erst auf der Ebene der Datenauswertung ergibt und nicht schon bei der Erhebung.[20]

Die Frage, die im Zusammenhang mit dieser Technik im Raum steht, ist, wie garantiert werden kann, dass nur die relevanten Daten gelesen und übermittelt werden, und ob dies überhaupt möglich ist. Ein Problem, welches durch die Nutzung zur Online-Durchsuchung entsteht, ist die Möglichkeit, dass sich ein unbefugter Dritter dazwischenschaltet oder (viel einfacher), dass sich dieser Unbefugte die Sicherheitslücken ebenfalls zu Nutzen macht, welches ein weiteres, ungleich schwereres Problem darstellt. Unbeabsichtigte Folgen der Infiltration können ebenfalls auftreten, indem der Betroffene, auf dessen informationstechnisches System eine entsprechende Software aufgespielt wurde, diese (versehentlich) an unbeteiligte Dritte weiterleitet. Eine weitreichende Ausführung zu den Sicherheitslücken und unbeabsichtigten Folgen der Infiltration fällt unter 2.3.3.

[20] Rehak, 2011 [25, S. 27]

2.3 Präventive Online-Durchsuchung (§ 49 BKAG, § 45 PAG Bayern)

Bei der präventiven Online-Durchsuchung handelt es sich um einen verdeckten Zugriff auf informationstechnische Systeme zu präventiven Zwecken, um Gefahren abzuwehren und Straftaten zu verhindern. Auf Bundesebene ist dieser Zugriff in § 49 BKAG geregelt, zugehörig dem Abschnitt 5 des BKAG, der die Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus enthält.

Nach § 5 BKAG erhält das Bundeskriminalamt die Aufgabe, Gefahren des internationalen Terrorismus abzuwehren, wenn die Gefahr länderübergreifend besteht, eine nicht erkennbare Zuständigkeit einer Landespolizeibehörde vorliegt oder die zuständige Landesbehörde um eine Übernahme ersucht.

2.3.1 Wörtliche Auslegung

Das Bundeskriminalamt kann mit technischen Mitteln einen Eingriff in die informationstechnischen Systeme einer Person vornehmen sowie Daten erheben, ohne dass die betreffende Person über den Eingriff informiert wird, heißt es in § 49 I BKAG. Voraussetzung dafür ist, dass aufgrund von bestimmten Tatsachen angenommen werden kann, dass eine Gefahr für ein „überragend wichtiges Rechtsgut“[21] , also eine Gefahr für Leib, Leben oder die Freiheit einer Person vorliegt oder eine Gefahr für Güter der Allgemeinheit, bei welchen durch eine Bedrohung Grundlagen oder Bestand von Bund oder Ländern oder Existenzgrundlagen der Menschen tangiert, bzw. angegriffen werden. Für die Zulässigkeit der Maßnahme reicht es aus, dass durch bestimmte Tatsachen die gerechtfertigte Annahme besteht, dass in einem überschaubaren Zeitrahmen zuvor genannte Rechtsgüter „auf eine zumindest ihrer Art nach konkretisierte Weise“ geschädigt werden; eine konkrete Wahrscheinlichkeit hinsichtlich der Schädigung der Rechtsgüter aufgrund des individuellen Verhaltens einer Person und innerhalb eines überschaubaren Zeitrahmens ist ebenfalls ausreichend. Die Maßnahme muss verhältnismäßig sein, also zur Erfüllung der Aufgabe dienen, Gefahren des internationalen Terrorismus nach § 5 abzuwehren, während keine andere Maßnahme als weniger eingriffsintensives Mittel den Zweck in ausreichender Weise erfüllen kann, die Erfüllung der Aufgabe also „aussichtslos oder wesentlich erschwert“ wäre.

Abs. 2 regelt, dass technisch sichergestellt werden soll, dass nur für die Datenerhebung unerlässliche Veränderungen vorgenommen werden und diese Veränderungen im Anschluss nach Beendigung der Maßnahme, soweit technisch möglich, automatisiert rück-

[21] BVerfG 27.2.2008 [14, Rn. 247]

gängig gemacht werden. Kopierte Daten sind dabei nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Die Maßnahme kann laut Abs. 3 auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen sind. Ansonsten darf sich die Maßnahme nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Damit die Online-Durchsuchung nach Abs. 1 durchgeführt werden kann, ist ein Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht notwendig, geregelt in Abs. 4 und 5. Nach Abs. 6 ist die Anordnung auf höchstens drei Monate zu befristen, Ausnahmen zur Verlängerung um jeweils bis zu drei Monate sind möglich. Abs. 7 regelt den Umgang mit dem Kernbereich privater Lebensgestaltung. So dürfen Daten, die unter diesen Kernbereich fallen, nicht verwertet werden und müssen unverzüglich gelöscht werden. Auch wird die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle festgelegt, so kommt dem anordnenden Gericht die Aufgabe zu, über Verwertbarkeit oder Löschung der erhobenen Daten zu entscheiden. Durch Abs. 8 kann das Bundeskriminalamt bei Gefahr im Verzug selbst die Initiative ergreifen und über die Erkenntnisverwertung, entsprechend dem gesetzten Rahmen, entscheiden. Die gerichtliche Entscheidung muss allerdings unverzüglich nachgeholt werden.

2.3.2 Systematische Auslegung

Auf Landesebene wurden ebenfalls gesetzliche Grundlagen zum heimlichen Zugriff auf informationstechnische Systeme geschaffen. Dabei geht diese Arbeit vor allem auf das Polizeiaufgabengesetz (PAG) Bayern ein, in welchem dieser Zugriff in § 45 geregelt wird. Diese Norm fällt in den dritten Abschnitt des PAGs, der sich mit der Datenverarbeitung auseinandersetzt, und befindet sich dort im zweiten Unterabschnitt mit den besonderen Befugnissen und Maßnahmen der Datenerhebung. Bayern ist mit seinem PAG ein Vorreiter auf der Länderebene in Bezug auf die Einführung der Online-Durchsuchung. Auch in weiteren Bundesländern ist eine gesetzliche Grundlage dieser Maßnahme bereits eingeführt worden, in anderen Bundesländern ist die Aufgabenausweitung der Polizei, bzw. Anpassung der Polizeigesetze an das BKAG in Arbeit.[22]

§ 45 PAG ist in seinen wesentlichen Zügen dem § 49 BKAG, vormals § 20k BKAG, nachempfunden. Mithilfe von technischen Mitteln ist ein verdeckter Zugriff auf ein informationstechnisches System und die anschließende Erhebung von Zugangsdaten und gespeicherten Daten seitens der Polizei unter gewissen Bedingungen erlaubt. Es bedarf einer Gefahr oder einer drohenden Gefahr für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, um auf das informationstechnische

[22] Frohne, 2018 [20]

System des Verantwortlichen zuzugreifen oder aber die Bedrohung eines bedeutenden Rechtsguts nach Art. 11 Abs. 3 Satz 2 Nr. 1 oder Nr. 2 PAG.

Nach § 45 PAG ist auch ein Zugriff auf das informationstechnische System von anderen Personen erlaubt, „soweit bestimmte Tatsachen die Annahme rechtfertigen, dass die unter Nr. 1 genannten Personen deren informationstechnischen Systeme benutzen oder benutzt haben und die Personen daher mutmaßlich in Zusammenhang mit der Gefahrenlage stehen." Im Vergleich zum BKAG wird hier ein direkter Zusammenhang hergestellt, dass Dritte aufgrund der Nutzung desselben informationstechnischen Systems in Zusammenhang mit der Gefahrensituation gebracht werden. Sowohl im BKAG als auch im PAG Bayern tritt selbst noch eine Regelung hinzu, dass Maßnahmen auch durchgeführt werden dürfen, wenn Dritte unvermeidbar betroffen seien (vgl. § 49 Abs. 3 BKAG und 45̃ Abs. 1 Satz 4 PAG). Bei dringender Gefahr ist nach § 45 Abs. 1 Satz 6 unter Einhaltung der Voraussetzungen das Löschen und auch Verändern von Daten erlaubt, wenn die Gefahr sich nicht anderweitig abwehren lässt. Ebenso ist durch § 45 Abs. 1 Satz 5 die Ermächtigung geschaffen, eine nicht offene Durchsuchung von Sachen durchzuführen und ebenfalls die Wohnung des Betroffenen verdeckt zu betreten und zu durchsuchen, sofern Erforderlichkeit hinsichtlich der Durchführung von Maßnahmen nach Abs. 1 oder Abs. 2 besteht.

2.3.3 Historische und teleologische Auslegung

Mit dem Gesetzesentwurf der Bundesregierung vom 20. August 2008 erhielt das Bundeskriminalamt für die Bekämpfung von Terrorismus zum ersten Mal die Aufgabe, Gefahren abzuwehren sowie entsprechende Befugnisse zur Umsetzung, um die Abwehr von Gefahren zu optimieren. Ein wesentlicher Vorteil der Entscheidung, die Gefahrenabwehr dem Bundeskriminalamt zuzuteilen, ist die Umgehung von möglichen Hürden in der Zuständigkeitsfrage, bzw. Aufspaltung der Zuständigkeit zwischen Bund und Ländern, sodass ein zeitnahes Handeln erfolgen kann, welches in Fällen hoher terroristischer Bedrohung sehr wichtig ist.[23] Durch die großflächige Verbreitung moderner Technologien können sich Straftäter jeglicher Art, so auch Personen im Bereich des internationalen Terrorismus, dieser Technologien bedienen und so den Auftrag und die wirksame Arbeit der Sicherheitsbehörden, Gefahren abzuwehren, vereiteln. In dem Zusammenhang sieht sich das Bundeskriminalamt konfrontiert mit „einer immer weiter verbreiteten Nutzung kryptografischer Verfahren, immer größer werdenden Datenmengen und den weit verbreiteten Möglichkeiten der mobilen Nutzung des Internets."[24] Um

[23] BT-Drs. 16/10121 [10, S. 16]
[24] BT-Drs. 16/10121 [10, S. 28]

den Gefahren krimineller Nutzung, die mit der Ausweitung technischer Möglichkeiten verbunden sind, entgegenzutreten und eine effektive Gefahrenabwehr möglich zu machen, erfordert es die Ausweitung der Befugnisse bzw. die Anpassung an die technischen Möglichkeiten durch die Schaffung gesetzlicher Grundlagen für Maßnahmen, die dem Bundeskriminalamt an die Hand gegeben werden können. Zu den Maßnahmen, mit denen sich das BKA dieser Konfrontation stellen will, gehört auch inzwischen die Online-Durchsuchung. Dabei orientiert sich die Bundesregierung in ihrem Gesetzesentwurf vom 20. August 2008 stark an dem vom Februar des gleichen Jahres stammenden Urteil des Bundesverfassungsgerichts bezogen auf das VSG Nordrhein-Westfalen, mit dem eine Grundlage für den heimlichen Zugriff auf informationstechnische Systeme geschaffen werden sollte. Das Bundesverfassungsgericht hat dabei eine solche Maßnahme bei Einhaltung bestimmter strenger Voraussetzungen für verfassungsrechtlich grundsätzlich zulässig erklärt.[25] So argumentierte das Bundesverfassungsgericht bereits in der Entscheidung zum nordrhein-westfälischen VSG vom Februar 2008, dass ein verdeckter Zugriff auf informationstechnische Systeme nur dann zulässig sei, wenn dieser Zugriff den näher genannten Forderungen entspreche, darunter Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthalte.[26] Die Formulierung eines neuen Wortlautes - eng an der Begründung des Bundesverfassungsgerichts zur Verfassungswidrigkeit dieser Maßnahme - führte nun dazu, dass durch die Übernahme dieses Gesetzesentwurfs die Online-Durchsuchung für präventive Zwecke eine gesetzliche Grundlage in § 20k BKAG erhielt und seit des Inkrafttretens der Neufassung des BKAGs am 1. Januar 2009, entsprechend den gesetzlichen Rahmenbedingungen, eingesetzt werden konnte.

Der große mit der Online-Durchsuchung einhergehende Vorteil ist die Heimlichkeit des Zugriffs, der Besitzer wird also nicht wie im Falle einer offenen Durchsuchung bzw. der physischen Beschlagnahme des informationstechnischen Systems gewarnt. Dementsprechend kann er auch keine Mittäter warnen und Daten von ermittlungstaktischem Wert vernichten. Ermittlungsansätze gehen dabei auch nicht verloren.[27] Ein weiterer Sinn, bestehend in der Heimlichkeit der Maßnahme, ist dem Einsetzen von Software zur Verschlüsselung seitens des Besitzers der informationstechnischen Systeme geschuldet. Dabei wird der Zugriff auf die gespeicherten und vorhandenen Daten durch eine Verschlüsselung von Teilen der Festplatte oder anderer Datenträger wesentlich erschwert oder ist gar unmöglich, wenn der Benutzer während der Beschlagnahme nicht gerade angemeldet ist und bleibt.[28]

Die Auffassung der sächsischen Staatsregierung - als Befürworter des ‚heimlichen Beob-

[25] BVerfG 20.4.2016 [15, Leitsatz 1. a)]
[26] BVerfG 27.2.2008 [14, Leitsätze 2, 3]
[27] Buermeyer [7, S. 34]
[28] Buermeyer [7, S. 35]

achten und sonstigen Aufklärens des Internets' in ihrer Stellungnahme zu den Verfassungsbeschwerden gegen das nordrhein-westfälische VSG aus dem Bundesverfassungsgerichtsurteil vom 02.02.2008 (speziell § 5 Abs. 2 Nr. 11 VSG), der Kernbereich privater Lebensgestaltung sei bei dem heimlichen Zugriff auf ein informationstechnisches System in Verbindung mit der Durchsicht und Überwachung sowie mit der Ausleitung und Übermittlung von Daten nicht betroffen, da „der Bürger zur höchstpersönlichen Kommunikation nicht auf einen Personalcomputer angewiesen sei,"[29] ist schon für das Jahr 2008 als veraltet zu betrachten und heutzutage kaum vorstellbar und nicht mehr zeitgemäß.

Moderne informationstechnische Systeme beinhalten ein äußerst umfassendes Abbild unseres Lebens in digitaler Form und „gleichen so einem ausgelagerten Teil des Gehirns." Durch die mögliche Reichweite der Ausspähung, die mit dem Zugriff einhergeht, können Ermittler den Besitzer des ausgespähten informationstechnischen Systems nicht selten besser kennen als der Besitzer sich selbst kenne.[30] Dies entspricht auch der Ansicht des Bundesverfassungsgerichts. So werden heutzutage durchaus u.a. auch tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente zunehmend in Dateiform angelegt.[31] Damit ist der Zugriff auf einen so umfassenden Datenbestand auch mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer gesamten Betrachtung weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.[32]

Diesbezüglich hat das Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 zu den anstehenden Verfassungsbeschwerden Stellung bezogen und bestätigt, dass der Einsatz von heimlichen Überwachungsmaßnahmen, so auch die Online-Durchsuchung nach § 20k BKAG zur Abwehr von Gefahren des internationalen Terrorismus im Grundsatz mit den Grundrechten kompatibel ist. Bei einer verfassungskonform einschränkenden Auslegung der Eingriffsvoraussetzungen sei dies mit der Verfassung vereinbar. [33] Allerdings seien die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung nicht ausreichend und somit verfassungswidrig.[34]

Innerhalb dieses Urteils setzte das Bundesverfassungsgericht ein Ultimatum, dass die für nicht vereinbar erklärten Vorschriften des BKAGs bis zum 30. Juni 2018 bzw. bis zu einer entsprechenden Neuregelung gelten. Im Februar 2017 wurde diese Neurege-

[29] BVerfG 27.2.2008 [14, Rn. 144]
[30] Buermeyer, 2017 [8, S. 5]
[31] BVerfG, 20.04.2016 [15, Rn. 210]
[32] BVerfG, 27.2.2008 [14, Rn. 232]
[33] BVerfG 20.4.2016 [15, Leitsatz 1. a); Rn. 211]
[34] BVerfG 20.4.2016 [15, Rn. 208]

lung entworfen, die im Mai 2018 in Kraft trat. Neben Änderungen zur Anpassung an die Datenschutz-Grundverordnung und das neue Bundesdatenschutzgesetz wurde u.a. auch der verdeckte Zugriff auf informationstechnische Systeme anders gefasst. Dabei entspricht § 49 dem alten § 20k weitestgehend. [35] Dennoch wurde § 49 an die kritisch beleuchteten Punkte aus dem Urteil vom 20. April 2016 angepasst. So befand das Bundesverfassungsgericht, dass die Auslegung von § 20k Abs. 1 Satz 2 BKAG verfassungskonform einschränkend sein müsse.[36] Um dennoch Unsicherheiten hinsichtlich der rechtlichen Anwendung der Maßnahme zu entgehen, wird die Gefahrenlage nun etwas enger gefasst. Des Weiteren wurde Abs. 5, der die Protokollierung des Einsatzes der Maßnahme regelte, entfernt, allerdings nur aufgrund der neuen Systematik des BKAGs, da mit § 82 BKAG eine zentrale Norm für die Protokollierung seitens des Bundeskriminalamtes bei dem Einsatz verdeckter Maßnahmen geschaffen wurde. Neu an die Stelle des Abs. 5 treten nun Anforderungen an den zu stellenden Antrag zur Durchführung der Maßnahme.[37]

In der Auffassung, Daten aus dem Kernbereich privater Lebensgestaltung dürften nicht verwertet werden und seien unmittelbar zu löschen sowie, dass nach technischen Möglichkeiten sicherzustellen sei, dass solche Daten gar nicht erst erhoben werden, enspricht § 49 Abs. 7 des neuen BKA-Gesetzes § 20k des alten BKA-Gesetzes und ist verfassungsrechtlich tragfähig hinsichtlich eines wirksamen Kernbereichschutzes.[38] Jedoch würden durch § 20k Abs. 7 Satz 3, 4 keine verfassungsrechtlich hinreichenden Vorkehrungen zum nachgelagerten Kernbereichsschutz getroffen, eine hinreichend unabhängige Kontrolle sei nicht auszumachen, so fällt die Sichtung weitgehend in die Hände der Mitarbeiter des Bundeskriminalamts.[39] Dem wirkt ein neu formulierter Teil des § 49 Abs. 7 entgegen, nach dem mittels einer Maßnahme nach Abs. 1 erlangte Daten unverzüglich dem anordnenden Gericht vorzulegen sind, welches ebenso unverzüglich über die Verwertbarkeit bzw. Löschung entscheidet. Nicht mit der Verfassung vereinbar sei laut Bundesverfassungsgerichtsurteil auch der zu kurze Zeitrahmen hinsichtlich der Aufbewahrung der Löschungsprotokolle gemäß § 20k Abs. 7 Satz 8 BKAG.[40] Dies wurde ebenfalls in § 49 BKAG angepasst, um die Effektivität der Ausübung der Betroffenenrechte sowie eine wirksame Kontrolle zu gewährleisten. Abs. 8 wird ergänzt und enthält für das Bundeskriminalamt die Möglichkeit, dass es in Ausnahmefällen, wenn Gefahr im Verzug ist, auch kurzfristig erste Handlungsmöglichkeiten erhält. [41]

[35] BT-Drs. 18/11163 [19, S. 118]
[36] BVerfG 20.4.2016 [15, Rn. 213]
[37] BT-Drs. 18/11163 [19, S. 118]
[38] BVerfG 20.4.2016 [15, Rn. 226]
[39] BVerfG 20.4.2016 [15, Rn. 223, 225]
[40] BVerfG 20.4.2016 [15, Rn. 226]
[41] BT-Drs. 18/11163 [19, S. 118]

Heimliche Überwachungsmaßnahmen, durchgeführt von staatlichen Stellen, erfordern Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung, welcher sich aus Art. 1 Abs. 1 GG ergibt, sofern dieser Kernbereich durch die Maßnahmen betroffen ist. Dieser Kernbereich ist selbst dann noch unantastbar in Form einer nicht zu rechtfertigenden Ausforschung, wenn „überwiegende Interessen der Allgemeinheit“ betroffen sind. „Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.“[42]

Bei dem heimlichen Zugriff auf informationstechnische Systeme ist es in den überwiegenden Fällen nicht zu vermeiden, dass Daten, die unter den Kernbereich privater Lebensgestaltung fallen, mit erhoben werden. Soweit möglich, sollen verfügbare informationstechnische Sicherungen das Erfassen von Daten mit Kernbereichsbezug verhindern. Während oder auch vor der Datenerhebung lässt sich der Kernbereichsbezug jedoch oft nicht bewerten, weshalb bei der Auswertung nun der Schutz zu Tragen kommt und so das Ausmaß der Verletzung des Kernbereichs privater Lebensgestaltung und ihre Auswirkungen so gering wie möglich gehalten werden sollen sowie die kernbereichsrelevanten Daten nicht verwertet und dazu unverzüglich gelöscht werden.[43] Wenn allein Informationen aus dem Kernbereich privater Lebensgestaltung erfasst werden, ist der Zugriff auf ein informationstechnisches System nicht erlaubt. Diese Formulierung sei laut Bundesverfassungsgericht verfassungsrechtlich gesehen tragfähig.[44] Wenn es jedoch konkrete Anhaltspunkte geben sollte, dass der Betroffene dem verdeckten Zugriff auf sein informationstechnisches System vorbeugt und Daten mit Kernbereichsbezug mit den dem Zweck der Ermittlung dienenden Daten verknüpft werden, so hat diese Maßnahme nicht grundsätzlich zu unterbleiben.[45] Grundsätzlich ist bei der Erfassung von den weitreichenden Datenbeständen, die sich heutzutage auf informationstechnischen Systemen befinden, schon im Vorfeld davon auszugehen, dass auch automatisch nicht kernbereichsrelevante Daten erfasst werden.

Dass Veränderungen im Anschluss nach Beendigung des Einsatzes der Online-Durchsuchung, *soweit technisch möglich*, automatisiert rückgängig gemacht werden, steht unter dem Vorbehalt technischer Realisierbarkeit.[46] Der Wortlaut ist auch hier bewusst „offen“ formuliert worden, da im Vorfeld nicht davon ausgegangen werden kann, dass sich die Veränderungen rückgängig machen lassen.

[42] BVerfG 27.2.2008 [14, Rn. 271]
[43] BVerfG 27.2.2008 [14, Rn. 277, 281, 282]
[44] BVerfG 20.4.2016 [15, Rn. 222]
[45] BVerfG 27.2.2008 [14, Rn. 281]
[46] Schmitt, in: Meyer-Goßner/Schmitt, 2018 [24, § 100a, Rn. 14l], auch auf Prävention anwendbar

Da die Maßnahme der Online-Durchsuchung (sowie auch andere Überwachungs- und Ermittlungsmaßnahmen mit je variierender Eingriffstiefe) in die Grundrechte eingreift und sie einschränkt, muss sie entsprechend am Verhältnismäßigkeitsgrundsatz ausgerichtet sein.[47] Dabei soll die Maßnahme ein gewisses Maß halten und nicht mehr als nötig in die Rechte des Betroffenen eingreifen, welches sich in der Legitimität, Geeignetheit, Erforderlichkeit und Angemessenheit widerspiegelt.[48] [49] Der Eingriff in die Grundrechte zur Ermöglichung der Online-Durchsuchung wiege schwer, aber verfolge mit dem Zweck der Abwehr von Gefahren des internationalen Terrorismus ein legitimes Ziel und sei zur Erreichung des Ziels sowohl geeignet als auch erforderlich, argumentiert das Bundesverfassungsgericht. [50] Auch hier ist damit eine offene Formulierung gewählt.

Neben der zu wahrenden Verhältnismäßigkeit und dem Kernbereichsschutz garantiert das allgemeine Persönlichkeitsrecht lückenschließend die Elemente, die bedeutend für die Persönlichkeit sind, aber nicht unter die besonderen Freiheitsgarantien des Grundgesetzes fallen. Die Notwendigkeit dieser Gewährleistung sieht das Bundesverfassungsgericht in neuartigen Gefährdungen, die sich aus dem technischen Fortschritt und aus mit der Zeit veränderten Lebensumstände durch die stets zunehmende Bedeutung der Nutzung informationstechnischer Systeme für die Entfaltung der Persönlichkeit ergeben. Aus dieser Entwicklung heraus hat sich ein Schutzbedürfnis entwickelt, dem der Staat durch die Wahrung der Integrität und Vertraulichkeit informationstechnischer Systeme als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)[51] gerecht werden will, sodass eine ungehinderte Entfaltung der Persönlichkeit jedes Einzelnen möglich ist.[52]

Die Integrität eines informationstechnischen Systems wird dann angegriffen, wenn unbefugte Dritte auf dieses System zugreifen und die Funktionen und Speicherinhalte nutzen können. Wenn dies vorliegt, ist „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen."[53] Neben dem Zugriff auf das System soll auch vor Einblicken Unbefugter, sei es durch den Staat oder durch unautorisierte Dritte, geschützt werden, dies fällt unter den Begriff der Vertraulichkeit.[54]

[47] BVerfG 20.4.2016 [15, Rn. 90]
[48] BVerfG 27.2.2008 [14, Rn. 218]
[49] Die Legitimität einer Maßnahme ergibt sich aus dem Zweck zur Umsetzung der Aufgaben, die dem Staat übertragen wurden. Geeignetheit ist gewährleistet, wenn Kausalität hinsichtlich des Zwecks besteht. Erforderlichkeit ist gegeben, wenn kein weniger eingriffsintensives Mittel zur Verfügung steht, um das Ziel zu erreichen. Angemessenheit ergibt sich aus der Schwere des Eingriff im Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe. Rehak [25, S. 43]
[50] BVerfG 20.4.2016 [15, Rn. 90]
[51] BVerfG 27.2.2008 [14, Rn. 169, 166]
[52] BVerfG 27.2.2008 [14, Rn. 181]
[53] BVerfG 27.2.2008 [14, Rn. 204]
[54] Hoffmann-Riem [22, S. 4]

Trotz des erklärten Schutzbedürfnisses gibt es keine schrankenlose Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. In das Grundrecht kann eingegriffen werden, wenn eine Rechtfertigung durch einen präventiven oder repressiven Zweck gegeben ist. Der Eingriff selbst muss aber verfassungsgemäß und gesetzlich geregelt sein."[55]

Sicherheitslücken

Wie schon die Bundesregierung in ihrem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 13. August 2008 berücksichtigte, hat der Staat die Aufgabe, die Sicherheit der Bevölkerung zu gewährleisten und dazu Gefahren für Leib, Leben und Freiheit abzuwenden.[56] Zu dieser Thematik äußerte sich weitergehend ebenfalls Hoffmann-Riem, dass Art. 10 GG die Telekommunikation vor unbefugtem Zugriff durch den Staat schütze, dieser aber selbst die Aufgabe besitze, die Telekommunikation, sowohl Inhalt als auch Umstände vor dem Zugriff privater Dritter zu schützen.[57] Dies gilt analog auch für die Online-Durchsuchung. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.[58]

Die unvergleichlich tiefen Einblicke in die Persönlichkeit des Betroffenen und der schwerwiegende Eingriff in seine Grundrechte machen den Einsatz von Trojanern „unvergleichlich heikel."[59] Damit die Spionagesoftware selbst überhaupt ausführbar ist, muss sie zunächst auf das zu infiltrierende System gelangen. Dies erfordert entweder eine Sicherheitslücke in dem betreffenden informationstechnischen System oder eine Lücke in seinen Schutzmechanismen. So werden die Behörden mit dem Problem konfrontiert, einerseits, wie schon zuvor aufgeführt, dem unbefugten Zugriff Dritter in informationstechnische Systeme vorzubeugen bzw. die Betroffenen entsprechend zu warnen, andererseits aber ihnen bekannte Sicherheitslücken nicht zu veröffentlichen, sodass sich diese zum Zweck des Aufspielens der Spionagesoftware verwenden lassen. Das Problem, welches damit einhergeht, ist, dass die Sicherheitslücken nicht nur bei den Behörden bekannt sind, davon kann zumindest ausgegangen werden.[60] Auf diesen Zielkonflikt verweist ebenfalls das Bundesverfassungsgericht in der Entscheidung über das nordrhein-

[55] BVerfG 27.2.2008 [14, Rn. 207]
[56] BT-Drs. 16/10121 [10, S. 28]
[57] Hoffmann-Riem [22, S. 6]
[58] BVerfG, 27.2.2008 [14, Rn. 181]
[59] Buermeyer, 2017 [8, S. 6]
[60] Hornung, 2007 [23, S. 580]; dazu auch CCC, 2017 [16, S. 8]

westfälische VSG. Es weist in diesem Zusammenhang auf die Gefahr hin, dass die Ermittlungsbehörde es unterlassen könne, die Schließung der entsprechenden Sicherheitslücken in die Wege zu leiten oder sogar gezielt dafür sorgt, dass diese Lücken unerkannt und damit bestehen bleiben.[61] Damit sei die Gefahr eines massiven Interesses seitens der Sicherheitsbehörden gegeben, die „Cyber-Sicherheit weltweit zu schwächen", so Buermeyer, der weiter auf den Ausbruch des *WannaCry*-Trojaners im Zusammenhang dieser „Kultur der kalkulierten IT-Unsicherheit" verweist. [62] Die NSA war über mehrere Jahre im Besitz von Informationen über die Sicherheitslücke ohne diese dem Softwarehersteller mitzuteilen, sodass sie hätte geschlossen werden können. Informationen zu dieser Sicherheitslücke gelangten jedoch an Unbekannte, die diese veröffentlichten. Bis zum Ausbruch konnten die Korrekturen des Softwareherstellers nicht mehr bei allen Systemen eingebunden werden.[63] Damit einher geht auch die Durchlöcherung oder gar Zerstörung des Vertrauens in die Sicherheit von IT-Infrastrukturen[64] und auch des Vertrauens in staatliche Behörden, für Sicherheit zu sorgen, statt diese durch ein solches Verhalten sogar noch zunichte zu machen.

Laut Äußerungen auf der offiziellen Internetseite des Bundeskriminalamts können keine näheren Auskünfte zu Entwicklungsständen und weiteren Details der Online-Durchsuchung als polizeiliches Einsatzmittel gegeben werden. Dies wird damit begründet, dass sich dadurch Rückschlüsse auf die technischen Fähigkeiten und Möglichkeiten des Bundeskriminalamts ziehen lassen und eine effektive Strafverfolgung und Gefahrenabwehr möglicherweise nicht mehr gewährleistet werden könne.[65] Hier ist aber auch zu erwähnen, dass es möglich ist, dass die Software für die Online-Durchsuchung nicht vom BKA selbst entwickelt wird. In dem Zusammenhang ist die Aussage des damaligen BKA-Präsidenten anzuführen, der am 19.10.2011 im Innenausschuss des Bundestages Folgendes verkündete: „Richtig ist, dass der Quellcode der Quellen-TKÜ-Software der Firma Digitask dem BKA nicht offen gelegt wurde. Auch die Quellcodes anderer kommerzieller Anbieter wurden dem BKA nicht offen gelegt." Die Software werde jedoch getestet und entsprechend ihrer Funktion geprüft, dass der Umfang nicht über die beim Hersteller beantragten Funktionen hinausgehe.[66] Ziercke bezog sich hier zwar auf die Quellen-Telekommunikationsüberwachung, dies lässt sich aber auch auf die Software der Online-Durchsuchung übertragen. Problematisch ist vor allem, dass die genannte Prüfung der Software „nur" nach bestem Wissen und Gewissen ausgeführt werden und ihrerseits auch eine Hintertür enthalten kann, die von Kriminellen mutwillig dort plat-

[61] BVerfG, 27.2.2008 [14, Rn. 241]
[62] Buermeyer, 2017 [8, S. 3]; Bezug zu § 100b StPO, aber auch bei Prävention zutreffend
[63] Buermeyer, 2017 [8, S. 6 f.]
[64] Hornung, 2007 [23, S. 580]
[65] BKA zur Online-Durchsuchung [9]
[66] Ziercke, 2011 [29, S. 12]

ziert wurde. Die Prüfung ist keine Garantie für das Finden von möglicherweise eingebauten Hintertüren.

In diesem Zusammenhang ist anzuführen, dass die Norm selbst den Schutz gegen unbefugte Nutzung nach dem Stand der Technik vorschreibt, verankert in § 100a Abs. 5 StPO. An dieser Stelle sind Bedenken zu äußern hinsichtlich der nicht präzisen Formulierung. Hier wird so auch offengelassen, wessen Software verwendet werden darf und welche konkreten Vorkehrungen getroffen werden müssen, um die Zuverlässigkeit der Beweiserhebung zu sichern. Zu begrüßen sei die ausschließliche Verwendung von staatlicher Software. Wenn Software von externen Anbietern verwendet werde, sei es von noch größerer Wichtigkeit, eine Zertifizierung durch eine unabhängige Stelle zu fordern.[67]

Auch wenn die staatliche Behörde die Funktion der Software in vollem Maße nachvollziehen und prüfen könnte und im Besitz des Quellcodes wäre, sodass dieser bei Gericht vorgelegt werden könnte, wären die konkreten Aktivitäten der Software zur Online-Durchsuchung nicht vollständig rekonstruierbar. Ein Grund dafür sei unter anderem die Interaktion mit einem komplexen informationstechnischen System, das es entweder zu infiltrieren gelte oder das bereits infiltriert sei. Die Zustände des Systems seien schon während der Durchführung der Maßnahme nicht im Detail bekannt. Die Dokumentation müsste ebenfalls auch alle im Nachhinein eingespielten Updates und Modifikationen einfassen, welches die Komplexität einer tatsächlichen Ablaufanalyse in einem außerordentlich hohen Maße steigere. Die Aktivitäten der Online-Durchsuchung auf dem infiltrierten System seien demzufolge auch nach Beenden der Maßnahme nicht rekonstruierbar.“[68]

Die zur Entscheidung über das nordrhein-westfälische VSG angehörten sachkundigen Auskunftspersonen haben ausgeführt, dass nicht ausgeschlossen werden könne, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht, sodass es durch Wechselwirkungen mit dem Betriebssystem zu Datenverlusten kommen könne. Auch sei zu berücksichtigen, dass ein lesender Zugriff allein aufgrund der Infiltration nicht gegeben sei. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können aufgrund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen. Dies kann den Betroffenen in vielfältiger Weise mit oder ohne Zusammenhang zu den Ermittlungen schädigen.[69] Auch lasse sich nicht ausschließen, dass der Betroffene, auf dessen System eine Spionagesoftware in Form eines vermeintlich nützlichen

[67] Roggan, 2017 [26, S. 824]

[68] Rehak, 2011 [25, S. 38]; Rehak spricht hier sogar von einer Steigerung der „Komplexität einer tatsächlichen Ablaufanalyse ins Unendliche.“

[69] BVerfG, 27.2.2008 [14, Rn. 240]

Programms aufgespielt wurde, dieses Programm unwissentlich an Dritte weitergibt und infolge dessen deren Systeme gegebenenfalls auch beschädigt werden.[70] Außerdem bestehe die Möglichkeit, dass der Betroffene die Online-Durchsuchung entdecke, in diesem Fall könne er die Untersuchungsergebnisse manipulieren und beeinflussen. Dadurch seien Originalität und Integrität der gefundenen Dokumente in Frage zu stellen.[71] Die Zuverlässigkeit der erhobenen Beweise sei ebenso problematisch durch die Anfälligkeit für Manipulationen Dritter.[72]

Das Problem, was sich nun daraus ergibt, ist, dass Dritte, die im Besitz von Sicherheitslücken sind, diese nicht nur an staatliche Behörden weitergeben, bzw. erstens an diese verkaufen, aber zweitens auch aufgrund von Profit die Schwachstellen mitunter an den Meistbietenden abgeben. So wird aus dem ursprünglichen Zweck des Einsatzes der Maßnahme, nämlich für Sicherheit zu sorgen, indem Gefahren abgewehrt werden, das Ergebnis genau zum Gegenteil, da die Unsicherheit der IT-Infrastruktur gefördert wird.

[70] BVerfG, 27.2.2008 [14, Rn. 241]
[71] Fox, 2007[18, S. 832]
[72] Schmitt, in: Meyer-Goßner/Schmitt, 2018 [24, § 100a, Rn. 14k]

2.4 Repressive Online-Durchsuchung (§ 100b StPO)

Bei der repressiven Online-Durchsuchung handelt es sich um einen verdeckten Eingriff auf informationstechnische Systeme zu repressiven Zwecken, um Straftaten aufzuklären und zu verfolgen. Die repressive Online-Durchsuchung wird in § 100b StPO geregelt.

2.4.1 Wörtliche Auslegung

Geregelt wird hier der Eingriff in ein informationstechnisches System durch den Einsatz technischer Mittel sowie die folgende Datenerhebung, wobei der Betroffene, der dieses System nutzt, nicht informiert werden muss. Voraussetzung dafür ist ein qualifizierter Verdacht durch die Gegebenheit „bestimmter Tatsachen“, dass jemand als Täter oder Teilnehmer eine in Abs. 2 bezeichnete besonders schwere Straftat begangen oder auch nur versucht hat zu begehen, sofern in diesen Fällen der Versuch strafbar ist, so Abs. 1 Satz 1. Die Tat muss auch im Einzelfall besonders schwer wiegen. Der Einsatz der Onlinedurchsuchung setzt ebenso voraus, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre, die repressive Maßnahme muss also auch verhältnismäßig sein.

Ein Katalog mit Straftaten, bei denen der Einsatz der Online-Durchsuchung zulässig ist, findet sich in Abs. 2. Abs. 3 regelt, dass sich die Onlinedurchsuchung nur gegen den Beschuldigten richten darf. Unter zwei Bedingungen ist jedoch ein Eingriff in informationstechnische Systeme anderer Personen zulässig. Dabei muss die Annahme aufgrund von bestimmten Tatsachen bestehen, dass der Beschuldigte informationstechnische Systeme der anderen Person benutzt, und die Durchführung des Eingriffs bei dem Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes von Mitbeschuldigten führen wird. Die Maßnahme darf auch eingesetzt werden, wenn andere Personen unvermeidbar betroffen sind. In Abs. 4 wird auf Regelungen in § 100a verwiesen, die analog angewendet werden können. Dies betrifft sowohl die technische Sicherstellung, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden müssen, als auch eine notwendige Protokollierung bei jedem Einsatz der Onlinedurchsuchung.

Der Kernbereich privater Lebensgestaltung wird nicht in § 100b StPO, sondern in § 100d StPO, zentral für die §§ 100a bis 100c, geregelt. Daneben finden sich in § 100e StPO zentrale Regelungen für das Verfahren bei diesen Maßnahmen.

2.4.2 Systematische Auslegung

Neben § 100b StPO gibt es keine weitere Regelung, die eine rechtliche Grundlage zum Einsetzen der Online-Durchsuchung zu repressiven Zwecken enthält.

2.4.3 Historische und teleologische Auslegung

Da informationstechnische Systeme in einem immer größer werdenden Rahmen eingesetzt werden und dementsprechend weit verbreitet sind, kommt ihnen eine entsprechend wichtige Rolle zu, nicht nur hinsichtlich der Gefahrenprävention, sondern auch im Hinblick auf die Aufklärung von Straftaten. So könne ein „lediglich fragmentarischer Strafrechtsschutz [...] kein Freibrief für technisch versierte Straftäter sein“[73], welche sich zu Nutze machen, dass ihre Taten mangels geeigneter Ermittlungsmaßnahmen der Behörden nicht effektiv verfolgt werden können. Die Idee der Waffengleichheit von Straftätern und Ermittlungsbehörden ist einleuchtend.

So wurden über die letzten Jahre zahlreiche Diskussionen hinsichtlich einer gesetzlichen Grundlage der Online-Durchsuchung zur Strafverfolgung geführt. Einige Stimmen sahen die Notwendigkeit der Schaffung einer gesetzlichen Grundlage zur Einsetzung der Maßnahme, für andere bestanden bereits gesetzliche Grundlagen. Wiederum andere sind der Ansicht, die inzwischen hinsichtlich gesetzlicher Grundlagen (bisher) verfassungsgemäße Online-Durchsuchung zu repressiven Zwecken sei nicht verhältnismäßig und ermögliche zu gravierende Eingriffe in die Rechte des Einzelnen, zumindest nach bisheriger Formulierung des Gesetzestextes.

Als Grundlage nicht verwendbar ist § 163 StPO (Aufgaben der Polizei im Ermittlungsverfahren) in Verbindung mit § 161 StPO (Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft) als Ermittlungsgeneralklauseln. Die Behörden und Beamten des Polizeidienstes haben zwar Straftaten zu erforschen sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Auch dürfen sie bei Feststellung der Rechtmäßigkeit durch das zuständige Amtsgericht mit technischen Mitteln personenbezogene Daten in oder aus einer Wohnung zu Beweiszwecken erlangen und verwenden, sofern die Verhältnismäßigkeit gegeben ist. Die Generalklausel in § 161 StPO schließt nur die Maßnahmen ein, deren Grundrechtseingriffe lediglich geringfügig sind.[74]

Auch lässt sich die Online-Durchsuchung nicht auf § 102, die Durchsuchung beim

[73] Czerner, 2017 [17]
[74] Hornung, 2007 [23, S. 576]

Beschuldigten, stützen, entgegen der Auffassung des Ermittlungsrichters des Bundesgerichtshofs im Beschluss vom 21.02.2006. Dieser hatte die Online-Durchsuchung eines Computers auf Grundlage des § 102 StPO für zulässig erkannt. In ihrer Anmerkung zu diesem Beschluss sehen Beulke und Meininghaus die Online-Durchsuchung jedoch als Zwangsmaßnahme an, welche aufgrunddessen erfordere, dass der Gesetzgeber dem Beschuldigten die in § 106 Abs. 1 StPO genannten Rechte, der Durchsuchung beiwohnen zu dürfen, gewähren müsse, um ihm gewisse Kontrollmöglichkeiten zu geben. Durch die Heimlichkeit verfalle jedoch diese Möglichkeit. Der Hinweis des BGH-Ermittlungsrichters, bei den §§107, 106 StPO handele es sich nach überwiegender Auffassung um „bloße Ordnungsvorschriften“[75] mit keinen Rechtsfolgen bei einem Verstoß, greife nicht.[76] Im November desselben Jahres hatte ein anderer Ermittlungsrichter die Zulässigkeit der Online-Durchsuchung auf Grundlage der StPO verneint.[77]

Demgegenüber schafft der dritte Strafsenat Klarheit, welcher mit dem Beschluss vom 31.01.2007, Daten auf der Festplatte eines informationstechnischen Systems online abzufragen, für unzulässig erklärt, da es keine bestehende Eingriffsermächtigung gebe, auf die man das Einsetzen dieser Maßnahme stützen könne, so auch nicht § 102 StPO.[78]

Andere Eingriffsnormen sind ebenfalls nicht als Grundlage für eine Online-Durchsuchung anzuwenden. § 100a StPO ist nicht einschlägig, da die Telekommunikation nur bei der Ausleitung des Systeminhalts über eine Leitung berührt wird. § 100c StPO greift ebenfalls nicht, da die Maßnahme das nichtöffentlich gesprochene Wort in einer Wohnung nicht einschließt. § 100f Abs. 1 Nr. 2 StPO gestattet lediglich den Einsatz technischer Mittel außerhalb der Wohnung.[79]

Um nun die Strafprozessordnung so zu ändern, dass sie ebenfalls eine Rechtsgrundlage für die Online-Durchsuchung enthält, statt wie bis dato nur für die offene Durchsuchung oder Beschlagnahme der auf informationstechnischen Geräte gespeicherter Daten nach §§ 94 ff., 102 ff. StPO sowie für die heimliche Telekommunikationsüberwachung § 100a, hat die Bundesregierung am 15. Mai 2017 eine Formulierungshilfe für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung zur Änderung der Strafprozessordnung und weiterer Gesetze[80] veröffentlicht, in dem die Online-Durchsuchung eine gesetzliche Grundlage erhält.[81] So wurde am 17. August 2017 die Online-Durchsuchung als § 100b StPO eingeführt, welche dann am 24. August 2017

[75] BGH, Ermittlungsrichter, 21.02.2006 - 3 BGs 31/06 [4, Rn. 12]
[76] Beulke/Meininghaus, 2007 [2, S. 60 ff.]
[77] BGH, Ermittlungsrichter, 25.11.2006 - 1 BGs 184/2006 [5]
[78] Bär, in Heintschel-Heinegg und Bockemühl, 2018 [6, Rn. 67]
[79] Hornung, 2007 [23, S. 576]
[80] Drucksache 18/11272
[81] Bundesregierung: Formulierungshilfe zu § 100b StPO [13, S. 1 ff.]

in Kraft getreten ist.

§ 100b StPO ist in seinem Aufbau dem § 100a StPO zur Telekommunikationsüberwachung und dem § 100c zur akustischen Wohnraumüberwachung sehr ähnlich hinsichtlich Eingriffsvoraussetzungen und Schranken. Ein Unterschied dabei jedoch ist, dass bei der Online-Durchsuchung wie bei der akustischen Wohnraumüberwachung eine besonders schwere Straftat erforderlich ist im Vergleich zu einer „lediglich" schweren Straftat bei der Telekommunikationsüberwachung. Der über den Anfangsverdacht hinausgehende qualifizierte Verdacht ist hingegen bei allen drei Maßnahmen erforderlich. Dabei greift § 100b StPO den Straftatenkatalog von § 100c StPO auf, bzw. ist dieser Katalog nach Änderung der StPO nun in § 100b Abs. 2 StPO aufgelistet, auf den § 100c Abs. 1 Nr. 1 StPO verweist. Der Katalog beinhaltet nicht nur Straftaten, bei denen das verletzte Rechtsgut und die angedrohte Strafe besonders schwer wiegen, sondern auch solche, die eine Komplexität der Beschaffung von Beweisen aufweisen und die Ermittler einen besonderen Aufklärungsbedarf begründet sehen.[82] Es sei zweifelhaft, ob bei Eigentums- und Vermögensdelikten die Straftaten als besonders schwer anzusehen seien, genauso auch nebenstrafrechtliche Delikte gegen das Asyl- und Aufenthaltsgesetz. Unter genauer Betrachtung seien die Legitimationsgründe nicht ausreichend, um einen so intensiven Grundrechtseingriff zu rechtfertigen.[83]

Auch in dem Zusammenhang ist die Ansicht des Ausschusses für Recht und Verbraucherschutz zu betrachten, dass das Bundeserfassungsgericht die Maßnahme der Online-Durchsuchung in ihrer Eingriffsintensität mit der einer Wohnraumüberwachung vergleiche.[84] Dabei äußerte sich das Bundesverfassungsgericht zum BKAG lediglich, dass die Intensität des Eingriffs in die Vertraulichkeit und Integrität informationstechnischer Systeme mit Eingriff in die Unverletzlichkeit der Wohnung vergleichbar sei.[85] Dieser kleine Unterschied führt jedoch dazu, dass die Eingriffsintensität von der Online-Durchsuchung und von der Wohnraumüberwachung auf die gleiche Stufe gestellt werden, wobei bei § 100c StPO letztlich auch „nur" die akustische Wohnraumüberwachung in der StPO zulässig ist. Bei Online-Durchsuchungen jedoch ist der Zugriff auf einen sehr umfassenden Datenbestand mit dem nahe liegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weit reichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen.[86] So übersteigt die Intensität des Eingriffs bei der Online-Durchsuchung die von Lauschangriffen, zumindest sei das, abhängig von der Ausgestaltung der Maßnah-

[82] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, Rn. 11]
[83] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, Rn. 11], ebenso Buermeyer, 2017 [8, S. 13]
[84] BT-Drs. 18/12785, 2017 [1, S. 54]
[85] BVerfG, 20.4.2016 [15, Rn. 210]
[86] BVerfG, 27.2.2008 [14, Rn. 232]

me möglich.[87] Die Eingriffsintensität sei nach der Auffassung Roggans eher mit heimlichen Hausdurchsuchungen vergleichbar, die sich auch wiederholt durchführen lassen.[88]

Buermeyer sieht die deutlich höhere Eingriffstiefe der Online-Durchsuchung im Vergleich zur akustischen Wohnraumüberwachung darin begründet, dass die Maßnahme neben der umfassenden heimlichen Auslesung der digitalen Daten, aufgrund derer sich Rückschlüsse auf die Persönlichkeit des Betroffenen ziehen lassen, auch beinhalte, dass sich Mikrofone und Kameras der informationstechnischen Systeme aktivieren lassen.[89] Bei der Online-Durchsuchung liegen die weitreichendsten Grundrechtseingriffe zugrunde, die die Strafprozessordnung zur Informationsgewinnung zulasse.[90]

Nach Schmitt ist das heimliche Aktivieren von Kameras und Mikrofonen jedoch nicht erlaubt. Zwar sei in der Gesetzesbegründung die Rede davon, dass das gesamte Nutzungsverhalten einer Person überwacht werden solle,[91] wovon das Nutzen von Kamerafunktionen grundsätzlich nicht ausgeschlossen werden könne. Auch sei die Aktivierung ein Eingriff in ein informationstechnisches System nach § 100b Abs. 1 Satz 1 StPO. Der Gesetzeswortlaut, es dürfen Daten „daraus“ erhoben werden, spreche allerdings gegen ein aktive Nutzung von Kamera und Mikrofon, dies werde von der Verwendung des Begriffs „Durchsuchung“ noch betont.[92] In Bezug darauf sieht Eschelbach das Aktivieren von Mikrofonen und Kameras wieder als zulässig an, da der Wortlaut dies seiner Auffassung nach nicht ausschließe, da akustische und optische Signale auch nichts anderes als Daten darstellen, die sich auf dem informationstechnischen System befinden und *aus diesem heraus* an die entsprechende Behörde weitergeleitet werden können.[93] Auch unter Vernachlässigung von Mikrofon und Kamera, fällt die Eingriffstiefe dennoch sehr hoch aus und so ist Buermeyer zuzustimmen, wenn er sagt, dass die Online-Durchsuchung biete ein „totalitäres Potential“[94], da eine Erfassung von personenbezogenen Daten des Betroffenen oder Dritter in größtmöglichem Umfang technisch realisierbar sei.[95] In dem Zusammenhang weist Buermeyer auf die geltende Unschuldsvermutung hin.[96]

Eine Abgrenzung zur akkustischen Wohnraumüberwachung ist im Gesetzestext ebenfalls gegeben, da eine Maßnahme nach § 100c StPO nur zulässig ist, wenn die Annahme aufgrund tatsächlicher Anhaltspunkte besteht, dass durch den Einsatz Äußerungen des

[87] Roggan, 2017 [26, S. 9]
[88] Roggan, 2017 [26, S. 7]
[89] Buermeyer, 2017 [8, S. 5 f.]
[90] Buermeyer, 2017 [8, S. 4]
[91] BT-Drs. 18/12875 [1, S. 59]
[92] Schmitt, in: Meyer-Goßner/Schmitt, 2018 [24, § 100b Rn. 2]
[93] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, Rn. 4]
[94] Buermeyer, 2017 [8, S. 4]
[95] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, Rn. 2]
[96] Buermeyer, 2017 [8, S. 5]

Beschuldigten erfasst werden, die für das Verfahren relevant sind. Roggan äußerte sich dazu kritisch, dass eine „Erfolgsprognose“ in diesem Sinne bei der Online-Durchsuchung nicht als notwendig angesehen werde, da davon ausgegangen werde, dass die ausgeleiteten Daten „immer“ auch verfahrensrelevante Informationen beinhalten.“[97]

Außerdem sei bedenklich, dass die Subsidiarität, die als Ausprägung des Verhältnismäßigkeitsgrundsatzes zu sehen sei und die im Vergleich zu den beiden anderen genannten Normen mit ähnlicher Geeignetheit für den Erfolg der Ermittlungen durch den Einsatz dieser Maßnahme vorausgesetzt werde, einen Beurteilungsspielraum entstehen lasse, der sehr vage erscheine.[98] Da die Eingriffstiefe der Online-Durchsuchung über die der akustischen Wohnraumüberwachung hinausgehen dürfte,[99] ist nun auch die höhere Schranke der Subsidiarität bei letzterer nicht nachzuvollziehen. Statt „nur“wesentlich erschwert, wie bei §§ 100a Abs. 1 Satz 3, 100b Abs. 1 Satz 3 StPO muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise *unverhältnismäßig* erschwert oder aussichtslos sein.

Ein weiterer Unterschied des § 100b zu § 100a StPO zeigt sich darin, dass sich die Online-Durchsuchung auch nur gegen andere Personen richten darf, wenn der Beschuldigte die informationstechnischen Systeme der anderen Person benutzt und auch nur dann, wenn der Eingriff bei dem Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führt, also sich als aussichtslos erweist. Bei der Telekommunikationsüberwachung reicht es, wenn bestimmte Tatsachen die Annahme rechtfertigen, „dass die betreffenden Personen für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte den Anschluss oder informationstechnische Systeme der Personen benutzt.“ In dieser Hinsicht ist die Voraussetzung für einen Eingriff der Online-Durchsuchung rechtlich enger gefasst.

Kritik erfährt § 100b StPO hinsichtlich seiner (zu geringen) Diskussion. An dieser Stelle ist anzuführen, dass der Begriff der Online-Durchsuchung im repressiven Zusammenhang erstmals wirklich in der Formulierungshilfe der Bundesregierung auftaucht, nicht etwa in dem Gesetzentwurf der Bundesregierung zur Änderung der Strafprozessordnung und weiterer Gesetze[100], auf die sich die Formulierungshilfe unmittelbar bezieht.

[97] Roggan, 2017 [26, S. 6]
[98] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, § 100b StPO Rn. 15]
[99] Schmitt, in: Meyer-Goßner/Schmitt, 2018 [24, § 100b StPO Rn. 2]
[100] BT-Drs. 18/11272

2.5 Übertragbarkeit der Argumente der präventiven auf die repressive Online-Durchsuchung

Zurzeit ist die Online-Durchsuchung sowohl zu präventiven als auch zu repressiven Zwecken, entsprechend der einzuhaltenden gesetzlichen Rahmenbedingungen, zulässig. Fraglich ist allerdings, ob sich die Argumente zwecks Gefahrenabwehr so einfach auf die Strafverfolgung übertragen lassen.

Aufgrund des hohen Gefahrenpotentials staatlicher Überwachungssysteme, dessen sich auch das Bundesverfassungsgericht bewusst war, leitete dieses in dem Urteil vom 27. Februar 2008 zum VSG des Landes Nordrhein-Westfalen und den darin geplanten Rechtsgrundlagen für Staatstrojaner das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ab.

Das Gewicht des Eingriffs in dieses Grundrecht ist von besonderer Intensität aufgrund der heimlichen technischen Infiltration und der damit einhergehenden Möglichkeit, über längere Zeit ein informationstechnisches System zu überwachen und die sich auf diesem System befindenden Daten zu erheben und auszuleiten.[101] Schon aber wegen der höchstpersönlichen Natur dieser Daten ist der Eingriff in das Grundrecht von besonderer Schwere.[102]

Aufgrund dieser Intensität muss die Maßnahme die vorgegebenen strengen Anforderungen einhalten, um eingesetzt werden zu können. Der Grundrechtseingriff entspricht nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Auch müssen geeignete Verfahrensvorkehrungen getroffen werden, um den Grundrechtsschutz für den Betroffenen zu sichern.[103] Im Umkehrschluss bedeutet dies, dass eine solche staatliche Maßnahme bei anderen, nicht überragend wichtigen Rechtsgütern Einzelner oder der Allgemeinheit nicht angemessen und nicht zu rechtfertigen ist. Zum Schutz dieser Rechtsgüter muss auf andere Ermittlungsbefugnisse zurückgegriffen werden.[104]

Schranken-Transfer

Dabei ist zu berücksichtigen, dass das Bundesverfassungsgericht nur auf den präventiven Zweck von Online-Durchsuchungen eingeht, sowohl in der Entscheidung zum

[101] BVerfG, 27.2.2018 [14, Rn. 234]
[102] BVerfG, 20.4.2016 [15, Rn. 210]
[103] BVerfG, 27.2.2008 [14, Rn. 242]
[104] Buermeyer, 2017 [8, S. 7 ff.]

nordrhein-westfälischen VSG als auch in der Entscheidung zu § 20k des alten BKAGs. Wie bereits in vorangegangenen Kapiteln erwähnt, ist dieses Grundrecht nicht schrankenlos, sodass Eingriffe zu präventiven und auch zu repressiven Zwecken zulässig sein können.[105] Dennoch lassen sich die Eingriffsschwellen nicht so leicht übertragen. Bei präventiven Maßnahmen steht der Schutz von (hier überragend wichtigen) Rechtsgütern im Vordergrund, eine Abwendung der Rechtsgüterverletzung ist also noch möglich. Die repressive Maßnahme regelt jedoch primär „nur" der Durchsetzung des staatlichen Strafanspruchs. Zwar dient dies am Ende auch nur dem Schutz von Rechtsgütern, Buermeyer spricht hier von „Meta-Rechtsgut", dennoch lässt sich die Rechtsgüterverletzung nicht mehr verhindern oder ungeschehen machen und daher dürfen im Vergleich zu präventiven Eingriffen keine geringeren Anforderungen an Eingriffe in die Integrität und Vertraulichkeit informationstechnischer Systeme zu repressiven Zwecken gestellt werden, im Hinblick auf den verfolgten Rechtsgüterschutz seien sogar eher höhere Anforderungen zu wählen.[106]

Hier lässt sich noch einmal aufgreifen, dass das Bundesverfassungsgericht ausdrücklich das Bestehen einer Gefahr für überragend wichtige Rechtsgüter zur Rechtfertigung des Einsatzes der Online-Durchsuchung (zu präventiven Zwecken) fordert und diese Gefahr im Einzelfall besonders schwer wiegen muss.[107] In diesem Zusammenhang sei es äußerst zweifelhaft, ob die Legitimationsgründe, vor allem von Eigentums- und Vermögensdelikten und erst recht von nebenstrafrechtlichen Delikten nach dem Asylgesetz oder dem Aufenthaltsgesetz, die sich im Straftatenkatalog von § 100b StPO finden, ausreichend seien, um einen so intensiven Grundrechtseingriff zu rechtfertigen.[108]

Zeitplan

Hier steht besonders die Kritik Buermeyers im Vordergrund, dass eine Maßnahme wie die Online-Durchsuchung, die die Grundrechte so stark einschränkt, parlamentarisch sowie außerparlamentarisch genügend diskutiert werden müsse, was nicht zu erkennen sei. So riet er im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages im Mai 2017 dazu, den Gesetzesentwurfs hinsichtlich der problematischen Aspekte zu überarbeiten und in der 19. Wahlperiode wieder aufzugreifen in Bezug auf Beratung und Diskussion, zumal diese Verzögerung kaum Auswirkungen auf die Praxis habe. [109]

[105] BVerfG, 27.2.2018 [14, Rn. 207]
[106] Buermeyer, 2017 [8, S. 10 f.]
[107] Bundesverfassungsgericht, 27.2.2008 [14, Rn. 242]
[108] Eschelbach, in: Satzger/Schluckebier/Widmaier, 2018 [28, Rn. 11], ebenso Buermeyer, 2017 [8, S. 13]
[109] Buermeyer, 2017 [8, S. 26]

Zudem lasse sich keine Rechtfertigung des Zeitdrucks erkennen. Weiter führt Buermeyer an, dass im Fokus stehe, Erkenntnisse mittels Verwendung der Maßnahme früher und heimlich zu erhalten, es gehe weniger um das Erhalten überhaupt. Kritischer zu betrachten ist jedoch seine Ausführung, dass sich die überwiegende Menge an Erkenntnissen aus der Online-Durchsuchung (und auch der Quellen-TKÜ) auch aus beschlagnahmten Systemen und dem darauffolgenden Zugriff und der Auswertung gewinnen lasse. [110] Diese Möglichkeit besteht zwar, aber die Verschlüsselung von für das Verfahren wichtigen Daten ist dennoch ein großes Hindernis, welches letztendlich einer effektiven Strafverfolgung im Weg stehen kann, zumal ein versierter Straftäter an die Verschlüsselung von relevanten Daten auf seinen informationstechnischen Systemen denken wird.

Im Zusammenhang mit der Regelung des Einsatzes der Online-Durchsuchung bei Gefahr im Verzug, verankert in § 100e Abs. 2 StPO, ist kritisch zu sehen, ob die Maßnahme unter Berücksichtigung des erheblichen Zeitaufwands der Vorbereitung einer Online-Durchsuchung mit den zu gewährleistenden technischen Voraussetzungen anwendbar sein dürfte.[111]

Beweisverwertung

Die Beweiskraft der ausgeleiteten Daten ist zu hinterfragen. Dies folgt aus der Art der Gewinnung der Daten. Überdies können die Daten manipuliert sein, falls der Beschuldigte den heimlichen Zugriff bemerkt und seine Daten entsprechend modifiziert, um die Ermittlungsbehörden zu täuschen. Durch das Aufspielen der Software kann es ebenfalls schon zu Veränderungen von Daten kommen. Die Verwendung von Sicherheitslücken zum Aufspielen der Software führt dazu, dass auch Dritte die Schwachstelle nutzen und ebenfalls Daten gezielt oder auch versehentlich verändern können. (Auch denkbar ist ein Angriff auf die Ermittlungsbehörden über den Übertragungswert.) Die Verwendung von Software kommerzieller Anbieter ist kritisch zu sehen, wenn der Quellcode den Ermittlungsbehörden oder dem Gericht nicht vorliegt und demzufolge nicht auf unerwünschte Nebenwirkungen geprüft werden kann.

[110] Buermeyer, 2017 [8, S. 25]
[111] dazu Roggan, 2017 [26, S. 9]

3 Zusammenfassung

Die Online-Durchsuchung hat in den letzten Jahren zunehmend an Aufmerksamkeit gewonnen und bietet viel Potenzial im Hinblick auf die Verhinderung von schweren Straftaten, bzw. Schadensbegrenzung, aber auch bezogen auf die Strafverfolgung. Dem gegenüber steht das Modell des gläsernen Menschen und die Frage, wie stark in die Persönlichkeitsrechte des Einzelnen eingegriffen werden kann und darf, um das Gemeinwohl zu schützen und die Frage, inwieweit es gerechtfertigt und verhältnismäßig ist, Sicherheitslücken bewusst offen zu lassen, um sie für diese Zwecke zu nutzen, gleichzeitig aber auch anderen das Tor offen zu halten. Stichwort: Informationstechnisches System als Speicher für ausgelagerten Teil unseres Gehirns

Als Online-Durchsuchung wird der verdeckte Zugriff auf ein informationstechnisches System bezeichnet. Dabei ist sowohl eine (einmalige) Durchsicht möglich, aber auch eine kontinuierliche Überwachung. Vor allem Letzteres bietet Vorteile in Bezug auf die Umgehung der Verschlüsselung von Teilen des informationstechnischen Systems. Die Maßnahme ist kein „Mehr“ zur Quellen-Telekommunikationsüberwachung, sie ermöglicht den Zugriff auf Daten, die nicht, noch nicht oder nicht mehr Gegenstand einer laufenden Telekommunikation sind. Durch die Unterscheidung sind sie an unterschiedlichen Grundrechten zu messen. Dabei ist für die Online-Durchsuchung allein das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme relevant.

Um nun auf die Daten eines informationstechnischen Systems zugreifen zu können, muss die Software zunächst auf dieses System aufgespielt werden. Dabei gibt es verschiedene Möglichkeiten. Die Software versteckt dabei ihren eigentlichen Zweck, um die Heimlichkeit der Maßnahme nicht zu gefährden.

Die Online-Durchsuchung kann sowohl zu präventiven als auch zu repressiven Zwecken durchgeführt werden. Auf Bundesebene ist die Verwendung zur Prävention in § 49 BKAG geregelt, auf Länderebene in verschiedenen Polizeigesetzen. Dabei muss aufgrund von bestimmten Tatsachen angenommen werden können, dass eine Gefahr für ein überragend wichtiges Rechtsgut vorliegt. Die Maßnahme muss verhältnismäßig sein und muss Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthalten. Dieser Schutz innerhalb des Gesetzes, damals noch § 20k BKAG, wurde in der Entscheidung des Bundesverfassungsgerichts von 2016 als nicht ausreichend angesehen, sodass eine Neuregelung erfolgte, um diese Maßnahme weiterhin einsetzen zu können.

Die Verwendung von (vor allem nicht öffentlich bekannten) Sicherheitslücken führt zu einem Zielkonflikt der staatlichen Behörden, einerseits informationstechnische Systeme

vor dem Zugriff von unbefugten Dritten zu schützen, andererseits ihnen bekannte Sicherheitslücken nicht zu veröffentlichen, bzw. an den Hersteller weiterzuleiten, um diese Sicherheitslücken für ihre Zwecke, z.B. für den Einsatz Online-Durchsuchung nutzen zu können. Darin besteht die Gefahr eines großen Interesses seitens der Sicherheitsbehörden, die Cyber-Sicherheit weltweit lückenhaft zu halten. Neben der Verwendung von Sicherheitslücken ist ebenfalls die Rekonstruierbarkeit der Durchführung und Funktion der Online-Durchsuchung problematisch. Vor allem, wenn verwendete Software nicht selbst vom BKA oder anderen staatlichen Stellen entwickelt wird, kann nicht in vollem Maße ausgeschlossen werden, dass die Softwareentwickler keine Hintertür eingebaut haben. So können unbefugte Dritte ebenfalls Zugriff auf das informationstechnische System des Betroffenen erhalten, auf welches die Spionagesoftware aufgespielt wurde. Der Betroffene kann unwissend diese Software auch an andere Personen weiterleiten oder aber die Software bemerken und so Untersuchungsergebnisse gezielt manipulieren.

Die repressive Online-Durchsuchung wird seit 2017 in § 100b StPO geregelt. Zavor gab es keine Rechtsgrundlage für eine Durchführung zu repressiven Zwecken. Die parlamentarische Diskussion erfolgte in keinem ausreichenden Umfang. Diese Norm hat dabei teilweise gleiche bis weiter gefasste Rahmenbedingungen im Vergleich zu §§ 100a, 100c StPO und auch zu § 49 BKAG. Nach einigen Aussagen biete sie „totalitäres Potential“.

Die Argumente der präventiven Online-Durchsuchung lassen sich teilweise auf die repressive übertragen. Dennoch gibt es ein paar Schwierigkeiten. So orientiert sich die Formulierung des Gesetzeswortlautes von § 100b StPO nah an dem Urteil des Bundesverfassungsgericht von 2016, und auch an dem Urteil von 2008. Bei diesen Entscheidungen steht allerdings der präventive Zweck im Vordergrund. Die Rechtsgutverletzung lässt sich noch verhindern. Wenn diese jedoch bereits eingetreten ist, dient die Online-Durchsuchung zwar auch mittelbar dem Rechtsgüterschutz, aber primär der Durchsetzung des Strafanspruchs. Daher sind keine geringeren Anforderungen an Eingriffe in das Computer-Grundrecht zu repressiven Zwecken zu stellen.

Die Beweiskraft der mittels Online-Durchsuchung erlangten Daten ist anzuzweifeln. Die Daten können versehentlich oder absichtlich durch Dritte, die Software oder den Betroffenen selbst verändert werden.

4 Fazit

So sehr es wünschenswert erscheint, Verbrechen zu verhindern, so schwierig gestaltet sich die Übertragbarkeit der Argumente der präventiven auf die repressive Online-Durchsuchung und der Umgang mit Sicherheitslücken sowie mit der zweifelhaften Beweiskraft erhaltener Erkenntnisse. Mit der präventiven Online-Durchsuchung ist den entsprechenden Behörden ein Werkzeug an die Hand gegeben worden zur Anpassung der Gefahrenabwehr an die gegebenen technischen Entwicklungen. Dadurch können Gefahren für überragend wichtige Rechtsgüter im besten Fall abgewendet werden. Zu beachten ist aber die Einhaltung des Schutzes des Kernbereichs privater Lebensgestaltung, wobei hier die gesetzlichen Rahmenbedingungen zum Teil relativ offen gehalten sind, welches unter anderem auch dadurch begründet werden kann, dass sich die Kernbereichsrelevanz bei der Datenerhebung meist noch nicht feststellen lässt.

Mit Vorsicht ist die Übertragung der Argumente der präventiven auf die repressive Online-Durchsuchung durchzuführen. Die gesetzliche Grundlage für diese richtet sich sehr nach den Bundesverfassungsgerichtsentscheidungen, die sich allerdings hauptsächlich auf den präventiven Zweck konzentrieren. Da bei dem präventiven Eingriff die Rechtsgüterverletzung noch verhindert werden kann, sollte der repressive Eingriff nicht weiter gefasst sein. Bei der Repression steht der Schutz von Rechtsgütern nur mittelbar im Vordergrund. Fraglich ist, ob die Erkenntnisse, die bei der repressiven Online-Durchsuchung gewonnen werden, vor Gericht Bestand haben. Der Grund liegt in der Veränderung von Daten durch die Software selbst, durch Dritte oder auch durch Betroffene. Wünschenswert ist die Weiterführung der parlamentarischen (und auch außerparlamentarischen) Diskussion und eine danach folgende Anpassung der Rahmenbedingugen. Auch ist keine Rechtfertigung des Zeitdrucks zu erkennen. Die Notwendigkeit der Ausgestaltung des Strafverfahrens ist zu sehen, dennoch sind die derzeitigen gesetzlichen Rahmenbedingungen zu weit gefasst. Auch wenn der Wunsch nach „Waffengleichheit“ eine schöne Vorstellung ist, führt kein Weg daran vorbei, den Umfang der Maßnahme einzuschränken.

Bei beiden Zwecken (sowohl Prävention als auch Repression) ist die Verwendung von Sicherheitslücken zum Aufspielen der Spionage-Software jedoch äußerst bedenklich, da so Dritten die Möglichkeit eröffnet wird, Schäden herbeizuführen. Problematisch ist der Zielkonflikt, der die Sicherheitsbehörden dazu verleitet, IT-Infrastruktur unsicher zu halten. Dies stellt einen Nebeneffekt der oben genannten Waffengleichheit dar.

Es bleibt ein Spagat zwischen Freiheit und Sicherheit.

5 Ausblick

Diese Arbeit zeigt einen Zwischenstand der (bisherigen) politischen und rechtlichen Entwicklung. Die weitere Entwicklung in Zukunft ist nicht ganz klar, abzusehen sind allerdings Verfassungsbeschwerden, die sich ihren Weg vor das Bundesverfassungsgericht bahnen, vor allem gegen die Online-Durchsuchung zum Zweck der Repression, wobei die Entscheidung noch offen ist. Weitere Widerstände werden sich gegen die Verschärfung der Polizeigesetze formieren. Da die Grundsätze des Vorgängers von § 49 BKAG bereits für zulässig, bzw. mit der Verfassung vereinbar erklärt wurden und auf die kritischen Aspekte in der Neuregelung eingegangen wurde, bleibt abzuwarten, ob Verfassungsbeschwerden diesbezüglich ebenfalls Anhörung finden, bzw. ihr Ziel erreichen.

Solange Sicherheitslücken zur Infiltration des informationstechnischen Systems verwendet werden, wird ein Interesse an einer unsicheren IT-Infrastruktur gegeben sein, das mit der Gefahr einhergeht, dass unbefugte Dritte ebenfalls Zugriff auf entsprechende informationstechnische Systeme erlangen können. Dies widerspricht im hohen Maße der Sicherheit von informationstechnischen Systemen, die auch in den Aufgabenbereich des Staates fällt. Durch die Unsicherheit der IT-Infrastruktur gefährdet der Staat somit möglicherweise seine Organe, bzw. sich selbst.

Vor dem Hintergrund, dass die „Five Eyes“ -Geheimdienste planen, Hersteller und Provider zu zwingen, Hintertüren einzubauen[112], scheint es eine noch weniger gute Perspektive für die Sicherheit hinsichtlich Integrität und Vertraulichkeit informationstechnischer Systeme und der damit einhergehenden freien Entfaltung der Persönlichkeit ohne Zugriff unbefugter Dritter zu geben.

Man darf gespannt sein, ob die Paradoxie, durch Sicherheitslücken zu mehr Sicherheit zu gelangen, aufgelöst werden kann und welche Richtung dabei eingeschlagen werden wird.

[112] Beuth, in: spiegel-online [3]

Erklärung

Hiermit versichere ich an Eides statt, dass ich meine Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Sprockhövel, den 01. Oktober 2018

_____

Annamaria Nockemann

A Anhang

A.1 § 49 BKAG

Nichtamtliches Inhaltsverzeichnis

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG)

§ 49 Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums die in Satz 1 genannten Rechtsgüter schädigen wird.

Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 5 erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.
(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.
(3) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.
(4) Die Maßnahme nach Absatz 1 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden.
(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme,
4. der Sachverhalt sowie
5. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.
(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, sind dem anordnenden Gericht unverzüglich vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach § 69 Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.
(8) Bei Gefahr im Verzug kann die Präsidentin oder der Präsident des Bundeskriminalamtes oder ihre oder seine Vertretung im Benehmen mit der oder dem Datenschutzbeauftragten des Bundeskriminalamtes über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie oder er sich der technischen Unterstützung von zwei weiteren Bediensteten des Bundeskriminalamtes bedienen, von denen einer die Befähigung zum Richteramt haben muss. Die Bediensteten des Bundeskriminalamtes sind zur Verschwiegenheit über die ihnen bekannt werdenden Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Absatz 7 ist unverzüglich nachzuholen.

Fußnote

(+++ § 49 Abs. 2: Zur Anwendung vgl. § 51 Abs. 2 +++)

A.2 § 45 PAG Bayern

PAG: Art. 45 Verdeckter Zugriff auf informationstechnische Systeme

Art. 45 Verdeckter Zugriff auf informationstechnische Systeme

(1) [1]Die Polizei kann mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben,

1. von den für eine Gefahr oder drohende Gefahr Verantwortlichen, soweit dies erforderlich ist zur Abwehr einer Gefahr oder einer drohenden Gefahr für ein in Art. 11 Abs. 3 Satz 2 Nr. 1 oder Nr. 2 genanntes bedeutendes Rechtsgut oder für Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, oder

2. von anderen Personen, soweit bestimmte Tatsachen die Annahme rechtfertigen, dass die unter Nr. 1 genannten Personen deren informationstechnischen Systeme benutzen oder benutzt haben und die Personen daher mutmaßlich in Zusammenhang mit der Gefahrenlage stehen.

[2]Auf informationstechnische Systeme und Speichermedien, die räumlich von dem von dem Betroffenen genutzten informationstechnischen System getrennt sind, darf die Maßnahme erstreckt werden, soweit von dem unmittelbar untersuchten informationstechnischen System aus auf sie zugegriffen werden kann oder diese für die Speicherung von Daten des Betroffenen genutzt werden. [3]Maßnahmen nach den Sätzen 1 und 2 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. [4]Sie dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. [5]Die eingesetzten Mittel sind entsprechend dem Stand der Technik gegen unbefugte Benutzung zu schützen. [6]Bei dringender Gefahr für ein in Satz 1 in Bezug genommenes Rechtsgut darf die Polizei Daten unter den übrigen Voraussetzungen des Satzes 1 löschen oder verändern, wenn die Gefahr nicht anders abgewehrt werden kann. [7]Im Übrigen dürfen Veränderungen am informationstechnischen System nur vorgenommen werden, wenn sie für die Datenerhebung unerlässlich sind. [8]Vorgenommene Veränderungen sind, soweit technisch möglich, automatisiert rückgängig zu machen, wenn die Maßnahme beendet wird.

(2) [1]Die Polizei kann unter den Voraussetzungen des Abs. 1 Satz 1 bis 5 auch technische Mittel einsetzen, um

1. zur Vorbereitung einer Maßnahme nach Abs. 1 spezifische Kennungen sowie

2. den Standort eines informationstechnischen Systems zu ermitteln.

[2]Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. [3]Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen. [4]Die Löschung ist zu dokumentieren.

(3) [1]Maßnahmen nach den Abs. 1 und 2 dürfen nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 36 Abs. 4 Satz 2 genannten Personen. [2]Die Anordnung der Maßnahmen ist schriftlich zu erlassen und zu begründen. [3]Die Anordnung muss, soweit möglich, Namen und Anschrift des Adressaten sowie die Bezeichnung des informationstechnischen Systems, auf das zugegriffen werden soll, enthalten. [4]In der Anordnung sind Art, Umfang und Dauer der Maßnahme zu bestimmen. [5]Die Anordnung darf auch zur nicht offenen Durchsuchung von Sachen sowie zum verdeckten Betreten und Durchsuchen der Wohnung des Betroffenen ermächtigen, soweit dies zur Durchführung von Maßnahmen nach Abs. 1 oder Abs. 2 erforderlich ist. [6]Die Anordnung ist einzelfallabhängig auf höchstens drei Monate zu befristen und kann um jeweils längstens drei Monate verlängert werden.

(4) Art. 41 Abs. 5 gilt für die durch Maßnahmen nach Abs. 1 erlangten personenbezogenen Daten entsprechend.

Literatur

[1] **Ausschuss für Recht und Verbraucherschutz (6. Ausschuss) der 18. Wahlperiode.** Drucksache 18/12785, *Beschlussempfehlung und Bericht*. (20.6.2017)

[2] **Beulke**, W., **Meininghaus**, F.: *Anmerkung zum Beschluss des BGH vom 21.02.2006, Az.: 3 BGs 31/06 (Heimliche Online-Durchsuchung eines PC)* StV, Heft 2, Seiten 60 - 65. (2007)

[3] **Beuth**, P.: *„Five Eyes" fordern freiwillige Hintertüren*. `http://www.spiegel.de/netzwelt/netzpolitik/five-eyes-\staaten-fordern-freiwillige-hintertueren-zur-ueberwachung-a-\1226463.html`, veröffentlicht am 04.09.2018, zuletzt abgerufen am 30.9.2018

[4] **BGH-Ermittlungsrichter** (Bearbeiter: Schlegel, S.): *BGH 3 BGs 31/06 - Zulässigkeit der verdeckte Durchsuchung eines Computersystems („Online-Durchsuchung"; Spionageprogramm)*. Beschluss vom 21.02.2006. HRRS 2007 Nr. 468. (2007)

[5] **BGH-Ermittlungsrichter** (Bearbeiter: Schlegel, S.): *BGH 1 BGs 184/2006 - (Kein) heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung („Online-Durchsuchung")*. Beschluss vom 25.11.2006. HRRS 2007 Nr. 466. (2007)

[6] **Bockemühl**, J., **Heintschel-Heinegg**, B.: KMR - Kommentar zur Strafprozessordnung. Carl Heymanns Verlag. (2018)

[7] **Buermeyer**, U.: *Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme*. HRRS, Ausgabe 4/2007, 8. Jahrgang, Seiten 154-166. (2007)

[8] **Buermeyer**, U.: *Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilf" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess*. Ausschuss-Drucksache 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages. (31.5.2017)

[9] **Bundeskriminalamt.** *Quellen-TKÜ und Online-Durchsuchung - Notwendigkeit, Sachstand und Rahmenbedingungen*. `https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html`, zuletzt abgerufen am 30.9.2018

[10] **Bundesregierung der 16. Wahlperiode.** Drucksache 16/10121, *Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*. (13.8.2008)

[11] **Bundesregierung der 18. Wahlperiode.** Drucksache 18/13031, *Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes.* (23.06.2017)

[12] **Bundesregierung der 18. Wahlperiode.** Drucksache 18/11272, *Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze*. (22.02.2017)

[13] **Bundesregierung der 18. Wahlperiode.** *Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze*, (15.5.2017)

[14] **Bundesverfassungsgericht.** *Bundesverfassungsgerichtsurteil des Ersten Senats vom 27. Februar 2008*. BVerfG, 1 BvR 370/07, 27.2.2008. `https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html`, zuletzt abgerufen am 30.09.2018

[15] **Bundesverfassungsgericht.** *Bundesverfassungsgerichtsurteil des Ersten Senats vom 20. April 2016*. BVerfG, 1 BvR 966/09, 20.4.2016. `https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html`, zuletzt abgerufen am 30.09.2018

[16] **Chaos Computer Club.** *Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung*. `https://www.ccc.de/system/uploads/227/original/Stellungnahme_CCC-Staatstrojaner.pdf`, zuletzt abgerufen am 30.09.2018

[17] **Czerner**, F.: *Digitale Forensik zwischen (Online-)Durchsuchung, Beschlagnahme und Datenschutz*. Kapitel 10 aus: Forensik in der digitalen Welt - Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Hrsg.: Labudde, D., Spranger, M. (2017)

[18] **Fox**, D.: *Realisierung, Grenzen und Möglichkeiten der „Online-Durchsuchung“* DuD, Ausgabe 31(?), Seiten 827 - 834. (2007)

[19] **Fraktionen der CDU/CSU und SPD der 18. Wahlperiode.** Drucksache 18/11163, *Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*. (14.2.2017)

[20] **Frohne**, K.: *Polizeigesetz - Befugnisse werden bundesweit ausgeweitet*. Frankfurter Rundschau, 15.5.2018. `http://www.fr.de/politik/polizeigesetz-befugnisse-werden-bundesweit-ausgeweitet-a-1505520`, zuletzt abgerufen am 30.9.2018

[21] **Graf**, J. P.: BeckOK StPO mit RiStBV und MiStra: Beck'scher Online-Kommentar. 30. Edition. C.H. Beck. (2018)

[22] **Hoffmann-Riem**, W.: *Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme*. JZ, 63. Jahrgang, Seiten 1009 – 1060. (2008)

[23] **Hornung**, G.: *Ermächtigungsgrundlage für die „Online-Durchsuchung“?* DuD, 31, Seiten 575 - 580 (2007)

[24] **Meyer-Goßner**, L., **Schmitt**, B.: Strafprozessordnung: StPO. 60. Aufl. C.H. Beck. (2018)

[25] **Rehak**, R.: *Angezapft - Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung* (2011 veröffentlicht; 2015 überarbeitet)

[26] **Roggan**, F.: *Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit für Beschuldigte und die Allgemeinheit*. StV - Strafverteidiger, Heft 12, Seiten 821 - 829. (2017)

[27] **Roßnagel**, A., **Skistims**, H.: *Rechtlicher Schutz vor Staatstrojanern - Verfassungsrechtliche Analyse einer Regierungsmalware* ZD 1/2012, Seiten 3 - 7. (2012)

[28] **Satzger**, H., **Schluckebier**, W., **Widmaier**, G.: Strafprozessordnung - Beck'sche Kurzkommentare. C.H. Beck. (2018)

[29] **Ziercke**, J.: *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)* (19.10.2011)